(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
8 March 2001 (08.03.2001)

PCT

(10) International Publication Number
WO 01/17251 A1

(51) International Patent Classification⁷: H04N 7/167

(21) International Application Number: PCT/US00/22785

(22) International Filing Date: 17 August 2000 (17.08.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/385,592 29 August 1999 (29.08.1999) US

(71) Applicant (*for all designated States except US*): INTEL CORPORATION [US/US]; 2200 Mission College Boulevard, Santa Clara, CA 95052 (US).

(72) Inventors; and
(75) Inventors/Applicants (*for US only*): GRAUNKE, Gary, L. [US/US]; 362 NE Hillwood Drive, Hillsboro, OR 97124 (US). LEE, David, A. [US/US]; 740 SW Willow Creek Drive, Beaverton, OR 97006 (US). FABER, Robert, W. [US/US]; 942 NE Third Avenue, Hillsboro, OR 97124 (US).

(74) Agents: MALLIE, Michael, J. et al.; Blakely, Sokoloff, Taylor & Zafman LLP, 7th floor, 12400 Wilshire Boulevard, Los Angeles, CA 90025 (US).

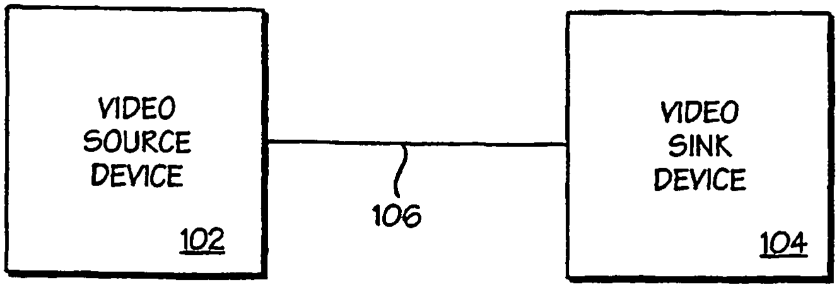
(81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: DIGITAL VIDEO CONTENT TRANSMISSION CIPHERING AND DECIPHERING MET HOD AND APPARATUS



(57) Abstract: A video source device generates a session key for each transmission session wherein a multi-frame video content is to be transmitted to a video sink device. The video source device uses the session key to generate a successive number of frame keys. The frame keys in turn are used to generate corresponding pseudo random bit sequences for ciphering the corresponding frames to protect the video content from unauthorized copying during transmission. The video sink device practices a complementary approach to decipher the received video content. In one embodiment, both devices are each provided with an integrated block/stream cipher to practice the transmission protection method.

Digital Video Content Transmission Ciphering And Deciphering Method And Apparatus

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to the field of content protection. More specifically, the present invention addresses the provision of protection to digital video content to facilitate their secure transmission from a video source device to a video sink device.

2. Background Information

In general, entertainment, education, art, and so forth (hereinafter collectively referred to as "content") packaged in digital form offer higher audio and video quality than their analog counterparts. However, content producers, especially those in the entertainment industry, are still reluctant in totally embracing the digital form. The primary reason being digital contents are particularly vulnerable to pirating. As unlike the analog form, where some amount quality degradation generally occurs with each copying, a pirated copy of digital content is virtually as good as the "gold master". As a result, much efforts have been spent by the industry in developing and adopting techniques to provide protection to the distribution and rendering of digital content.

Historically, the communication interface between a video source device (such as a personal computer) and a video sink device (such as a monitor) is an analog interface. Thus, very little focus has been given to providing protection for the transmission between the source and sink devices. With advances in integrated circuit and other related technologies, a new type of digital interface between video source and sink devices is emerging. The availability of this type of new digital interface presents yet another new challenge to protecting digital

Figure 5 illustrates the combined block/stream cipher of **Fig. 4** in further detail, in accordance with one embodiment;

Figure 6 illustrates the block key section of **Fig. 5** in further detail, in accordance with one embodiment;

Figure 7 illustrates the block data section of **Fig. 5** in further detail, in accordance with one embodiment; and

Figures 8a-8c illustrate the stream data section of **Fig. 5** in further detail, in accordance with one embodiment.

DETAILED DESCRIPTION OF THE INVENTION

In the following description, various aspects of the present invention will be described, and various details will be set forth in order to provide a thorough understanding of the present invention. However, it will be apparent to those skilled in the art that the present invention may be practiced with only some or all aspects of the present invention, and the present invention may be practiced without the specific details. In other instances, well known features are omitted or simplified in order not to obscure the present invention.

Various operations will be described as multiple discrete steps performed in turn in a manner that is most helpful in understanding the present invention. However, the order of description should not be construed as to imply that these operations are necessarily performed in the order they are presented, or even order dependent. Lastly, repeated usage of the phrase "in one embodiment" does not necessarily refer to the same embodiment, although it may.

Referring now to **Figure 1**, wherein a block diagram illustrating an overview of the present invention, in accordance with one embodiment is shown. As illustrated, video source device **102** and video sink device **104** are coupled to each other by digital video link **106**. Video source device **102** provides video content to video sink device **104** through digital video link **106**. In accordance

203). Upon exchanging the above information, source and sink devices **102** and **104** independently generate their respective copies of an authentication key (Km) using Ak and Bk (block **204** and **205**). For the illustrated embodiment, source device **102** generates its copy of Km by summing private keys of its provided array indexed by Bk, while sink device **104** generates its copy of Km by summing private keys of its provided array indexed by Ak. At this time, if both source and sink devices **102** and **104** are authorized devices, they both possess and share a common secret authentication key Km.

In one embodiment, each of source and sink devices **102** and **104** is pre-provided with an array of 40 56-bit private keys by the certification authority. An is a 64-bit random number, and Km is 56-bit long. For more information on the above described authentication process, see co-pending U.S. Patent Application, serial number 09/275,722, filed on March 24, 1999, entitled Method and Apparatus for the Generation of Cryptographic Keys, having common inventorship as well as assignee with the present application.

Having authenticated sink device **104**, source device **102** ciphers video content into a ciphered form before transmitting the video content to sink device **104**. Source device **102** ciphers the video content employing a symmetric ciphering/deciphering process, and using the random number (An) as well as the independently generated authentication key (Km) (block **206**). Upon receipt of the video content in ciphered form, sink device **104** deciphers the ciphered video content employing the same symmetric ciphering/deciphering processing, and using the provided An as well as its independently generated copy of Km (block **207**).

In accordance with the present invention, as an integral part of ciphering video content, source device **102** derives a set of verification reference values in a predetermined manner (block **208**). Likewise, as an integral part of symmetrically deciphering video content sink device **104** also derives a set of verification values in a predetermined manner, and transmits these derived verification values to source device **102** (block **209**). Upon receiving each of

Upon generating the session key Ks, source device **102** generates an initial version of a second random number (M0) (block **304**). For the illustrated embodiment, source device **102** first generates a pseudo random bit sequence (at p-bit per clock) using a stream cipher with the above described random number An and the session key Ks (in two roles, as another input random number and as the stream cipher key), applying C2 clocks. Source device **102** derives M0 from the pseudo random bit sequence, as the bit sequence is generated.

Next, source device **102** generates a frame key (Ki) for the next frame (block **306**). For the illustrated embodiment, Ki is generated by block ciphering an immediately preceding version of the second random number Mi-1 using the session key Ks as the block cipher key, and applying C3 clocks. That is, for the first frame, frame-1, frame key K1 is generated by block ciphering the above described initial version of the second random number M0, using Ks, and applying C3 clocks. Additionally, this operation is subsequently repeated at each vertical blanking interval for the then next frame, frame-2, frame-3, and so forth.

Upon generating the frame key Ki, source device **102** generates the current version of the second random number (Mi) (block **302**). For the illustrated embodiment, source device **102** first generates a pseudo random bit sequence (at p-bit per clock) using a stream cipher with the previous version of the second random number Mi-1 and the frame key Ki (in two roles, as another input random number and as the stream cipher key), applying C4 clocks. Source device **102** derives Mi from the pseudo random bit sequence, as the bit sequence is generated.

Upon generating the current version of the second random number Mi, source device **102** again generates a pseudo random bit sequence (at p-bit per clock) to cipher the frame (block **308**). For the illustrated embodiment, source device **102** generates the pseudo random bit sequence using a stream cipher with an immediately preceding version of the second random number Mi-1 and frame key Ki (in two roles, as another input random number and the stream are 56 clocks in length. Each 64-bit Mi is formed by concatenating the "lower" 16-bit stream cipher output of each of the last four clocks.

Accordingly, video content may be advantageously transmitted in ciphered form with increased robustness from source device **102** to sink device **104** through link **106** with reduced pirating risk.

Figure 4 illustrates video source and sink devices of **Fig. 1** in further detail, in accordance with one embodiment. As shown, video source and sink devices **102** and **104** include interfaces **108a** and **108b** disposed at the respective end of link **106**. Each of interfaces **108a** and **108b** is advantageously provided with cipher **110** of the present invention and XOR **112** to practice the video content protection method of the present invention as described above. Additionally, for ease of explanation, interface **108a** is also shown as having been provided with a separate random number generator **114**. Except for interfaces **108a** and **108b**, as stated earlier, video source and sink devices **102** and **104** are otherwise intended to represent a broad category of these devices known in the art.

Random number generator **114** is used to generate the earlier described random number An. Random number generator **114** may be implemented in hardware or software, in any one of a number of techniques known in the art. In alternate embodiments, as those skilled in the art will appreciate from the description to follow, cipher **110** may also used to generate An, without the employment of a separate random number generator.

Cipher **110** is a novel combined block/stream cipher capable of operating in either a block mode of operation or a stream mode of operation. To practice the video content protection method of the present invention, cipher **110** is used in block mode to generate the above described session key Ks and frame keys Ki, and in stream mode to generate the pseudo random bit sequences for the various frames (and indirectly Mi, as they are derived from the respective bit sequences).

intermediate "keys", which are stored away (in storage locations not shown). The stored intermediate "keys" are then applied to the ciphered text in reversed order, resulting in the deciphering of the ciphered text back into the original plain text. Another approach to deciphering the ciphered text will be described after block key section **502** and data section **504** have been further described in accordance with one embodiment each, referencing **Figs. 6-7**.

In stream mode, stream key section **506** is provided with a stream cipher key, such as the earlier described session key Ks or frame key Ki. Block key section **502** and data section **504** are provided with random numbers, such as the earlier described session/frame keys Ks/Ki and the derived random numbers Mi-1. "Rekeying enable" signal is set to an "enabled" state, operatively coupling block key section **502** to stream key section **506**. Periodically, at predetermined intervals, such as the earlier described horizontal blanking intervals, stream key section **506** is used to generate one or more data bits to dynamically modify the then current state of the random number stored in block data section **502**. During each clock cycle, in between the predetermined intervals, both random numbers stored in block key section **502** and data section **504** are transformed. The random number provided to block key section **502** is independently transformed, whereas transformation of the random number provided to data section **504** is dependent on the transformation being performed in block key section **502**. Mapping block **506** retrieves a subset each, of the newly transformed states of the two random numbers, and reduces them to generate one bit of the pseudo random bit sequence. Thus, in a desired number of clock cycles, a pseudo random bit sequence of a desired length is generated.

For the illustrated embodiment, by virtue of the employment of the "rekeying enable" signal, stream key section **506** may be left operating even during the block mode, as its outputs are effectively discarded by the "rekeying enable" signal (set in a "disabled" state).

Again, substitution boxes **604** and linear transformation unit **606** may be implemented in a variety of ways in accordance with well known cryptographic principles.

In one implementation for the above described embodiment, each register **602a**, **602b**, **602c**, **702a**, **702b**, **702c** is 28-bit wide. [Whenever registers **602a-602c** or **702a-702cb** collectively initialized with a key value or random number less than 84 bits, the less than 84-bit number is initialized to the lower order bit positions with the higher order bit positions zero filled.] Additionally, each set of substitution boxes **604** or **704** are constituted with seven 4 input by 4 output substitution boxes. Each linear transformation unit **606** or **706** produces 56 output values by combining outputs from eight diffusion networks (each producing seven outputs). More specifically, the operation of substitution boxes **604/704** and linear transformation unit **606/706** are specified by the four tables to follow. For substitution boxes **604/704**, the Ith input to box J is bit I*7+J of register **602a/702a**, and output I of box J goes to bit I*7+j of register **602c/702c**. [Bit 0 is the least significant bit.] For each diffusion network (linear transformation unit **606** as well as **706**), the inputs are generally labeled I0-I6 and the outputs are labeled O0-O6. The extra inputs for each diffusion network of the linear transformation unit **706** is labeled K0-K6.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
SK	8	14	5	9	3	0	12	6	1	11	15	2	4	7	10	13
SK	1	6	4	15	8	3	11	5	10	0	9	12	7	13	14	2
SK	13	11	8	6	7	4	2	15	1	12	14	0	10	3	9	5
SK	0	14	11	7	12	3	2	13	15	4	8	1	9	10	5	6
SK	12	7	15	8	11	14	1	4	6	10	3	5	0	9	13	2
SK	1	12	7	2	8	3	4	14	11	5	0	15	13	6	10	9
SK	10	7	6	1	0	14	3	13	12	9	11	2	15	5	4	8
SB	12	9	3	0	11	5	13	6	2	4	14	7	8	15	1	10
SB	3	8	14	1	5	2	11	13	10	4	9	7	6	15	12	0
SB	7	4	1	10	11	13	14	3	12	15	6	0	2	8	9	5
SB	6	3	1	4	10	12	15	2	5	14	11	8	9	7	0	13

I_5	Kz5	Kz8	Kz11	Kz14	Kz17	Kz20	Kz23	Kz26
I_6	Kz6	Kz9	Kz12	Kz15	Kz18	Kz21	Kz24	Kz27
O_0	Kx0	Ky0	Ky1	Ky2	Ky3	Kx7	Kx8	Kx9
O_1	Kx1	Ky4	Ky5	Ky6	Ky7	Kx10	Kx11	Kx12
O_2	Kx2	Ky8	Ky9	Ky10	Ky11	Kx13	Kx14	Kx15
O_3	Kx3	Ky12	Ky13	Ky14	Ky15	Kx16	Kx17	Kx18
O_4	Kx4	Ky16	Ky17	Ky18	Ky19	Kx19	Kx20	Kx21
O_5	Kx5	Ky20	Ky21	Ky22	Ky23	Kx22	Kx23	Kx24
O_6	Kx6	Ky24	Ky25	Ky26	Ky27	Kx25	Kx26	Kx27

Tables II & III – Diffusion networks for linear transformation unit **606/706** (continued in Table IV).

	B1	B2	B3	B4	B5	B6	B7	B8
I_0	Bz0	By0	By4	By8	By12	By16	By20	By24
I_1	Bz1	By1	By5	By9	By13	By17	By21	By25
I_2	Bz2	By2	By6	By10	By14	By18	By22	By26
I_3	Bz3	By3	By7	By11	By15	By19	By23	By27
I_4	Bz4	Bz7	Bz10	Bz13	Bz16	Bz19	Bz22	Bz25
I_5	Bz5	Bz8	Bz11	Bz14	Bz17	Bz20	Bz23	Bz26
I_6	Bz6	Bz9	Bz12	Bz15	Bz18	Bz21	Bz24	Bz27
K_0	Ky0	–	–	–	–	Ky7	Ky14	Ky21
K_1	Ky1	–	–	–	–	Ky8	Ky15	Ky22
K_2	Ky2	–	–	–	–	Ky9	Ky16	Ky23
K_3	Ky3	–	–	–	–	Ky10	Ky17	Ky24
K_4	Ky4	–	–	–	–	Ky11	Ky18	Ky25

combiner function **804**, coupled to each other as shown. LFSRs **802** are collectively initialized with a stream cipher key, e.g. earlier described frame key Ki. During operation, the stream cipher key is successively shifted through LFSRs **802**. Selective outputs are taken from LFSRs **802**, and combiner function **804** is used to combine the selective outputs. In stream mode (under which, rekeying is enabled), the combined result is used to dynamically modify a then current state of a block cipher key in block key section **502**.

For the illustrated embodiment, four LFSRs of different lengths are employed. Three sets of outputs are taken from the four LFSRs. The polynomials represented by the LFSR and the bit positions of the three sets of LFSR outputs are given by the table to follows:

LFSR	**Polynomial**	**Combining Function Taps**		
		0	**1**	**2**
3	$X^{17} + x^{15} + x^{11} + x^{5} + 1$	6	12	17
2	$X^{16} + x^{15} + x^{12} + x^{8} + x^{7} + x^{5} + 1$	6	10	16
1	$X^{14} + x^{11} + x^{10} + x^{7} + x^{6} + x^{4} + 1$	5	9	14
0	$X^{13} + x^{11} + x^{9} + x^{5} + 1$	4	8	13

Table V – Polynomials of the LFSR and tap positions.

The combined result is generated from the third set of LFSR outputs, using the first and second set of LFSR outputs as data and control inputs respectively to combiner function **802**. The third set of LFSR outputs are combined into a single bit. In stream mode (under which, rekeying is enabled), Referring now to back to **Figure 5**, as illustrated and described earlier, mapping function **508** generates the pseudo random bit sequence based on the contents of selected registers of block key section **502** and data section **504**. In one embodiment, where block key section **502** and data section **504** are implemented in accordance with the respective embodiments illustrated in **Fig. 6-7**, mapping function **508** generates the pseudo random bit sequence at 24-bit per clock based on the contents of registers (Ky and Kz) **602b-602c** and (By and Bz) **702b-702c**. More specifically, each of the 24 bits is generated by performing the XOR operation on nine terms in accordance with the following formula:

(B0•K0) ⊕ (B1•K1) ⊕ (B2•K2) ⊕ (B3•K3) ⊕ (B4•K4) ⊕ (B5•K5) ⊕ (B6•K6) ⊕ B7 ⊕ K7

Where "⊕" represents a logical XOR function, "•" represents a logical AND function, and the input values B and K for the 24 output bits are

Input	B0	B1	B2	B3	B4	B5	B6	B7	K0	K1	K2	K3	K4	K5	K6	K7
Origin	Bz	Bz	Bz	Bz	Bz	Bz	Bz	By	Kz	Kz	Kz	Kz	Kz	Kz	Kz	Ky
Outpu bit																
	14	23	7	27	3	18	8	20	12	24	0	9	16	7	20	13
	20	26	6	15	8	19	0	10	26	18	1	11	6	20	12	19
	7	20	2	10	19	14	26	17	1	22	8	13	7	16	25	3
	22	12	6	17	3	10	27	4	24	2	9	5	14	18	21	15
	22	24	14	18	7	1	9	21	19	24	20	8	13	6	3	5
	12	1	16	5	10	24	20	14	27	2	8	16	15	22	4	21
	5	3	27	8	17	15	21	12	14	23	16	10	27	1	7	17
	9	20	1	16	5	25	12	6	9	13	22	17	1	24	5	11
	23	25	11	13	17	1	6	22	25	21	18	15	6	11	1	10
	4	0	22	17	25	10	15	18	0	20	26	19	4	15	9	27
1	23	25	9	2	13	16	4	8	2	11	27	19	14	22	4	7
1	3	6	20	12	25	19	10	27	24	3	14	6	23	17	10	1
1	26	1	18	21	14	4	10	0	17	7	26	0	23	11	14	8
1	2	11	4	21	15	24	18	9	5	16	12	2	26	23	11	6
1	22	24	3	19	11	4	13	5	22	0	18	8	25	5	15	2
1	12	0	27	11	22	5	16	1	10	3	15	19	21	27	6	18

CLAIMS

What is claimed is:

1. In a video source device, a method comprising:
generating a session key for a transmission session within which a multi-frame video content is to be transmitted to a video sink device; and
generating a successive number of frame keys, using at least the session key, to facilitate ciphering of corresponding frames of the multi-frame video content for transmission to the video sink device.

2. The method of claim 1, wherein said generating of successive frame keys comprises generating at each vertical blanking interval of said multi-frame video content, a frame key for ciphering a frame of said multi-frame video content.

3. The method of claim 2, wherein said method further comprises generating a pseudo random bit sequence for each frame, using at least the corresponding frame key, for ciphering the particular frame of said multi-frame video content.

4. The method of claim 3, wherein each of said generating of a pseudo random bit sequence using a corresponding frame key comprises successive modifications of the corresponding frame key.

5. The method of claim 4, wherein said successive modifications of the corresponding frame key are performed at horizontal blanking intervals of the frame.

6. The method of claim 3, wherein said method further comprises generating an initial pseudo random bit sequence using at least the session key, and deriving an initial pseudo random number from the initial pseudo random bit sequence to be used with a first frame key to generate a first pseudo random bit sequence to cipher a first frame.

7. The method of claim 3, wherein each of said generating of a pseudo random bit sequence comprises generating sufficient number of pseudo random bits for ciphering a pixel on a bit-wise basis each clock.

8. In a video source device, a method comprising:
generating a frame key for each frame of a multi-frame video content; and
generating a pseudo random bit sequence for each of the corresponding frames, using at least the corresponding frame key, for ciphering the video content.

9. The method of claim 8, wherein said generating of a frame key for each frame comprises generating one frame key at each vertical blanking interval of said multi-frame video content.

17. The apparatus of claim 13, wherein the block cipher comprises a first and a second register to store a first and a second value, and a function block coupled to the first and second registers to transform the stored first and second values, with a selected one of the transformed first and second values being the session key or a frame key.

18. The apparatus of claim 17, wherein the block cipher is an integral part of said stream cipher.

19. In a video sink device, a method comprising:

generating a session key for a reception session within which a multi-frame video content is to be received from a video source device; and

generating a successive number of frame keys, using at least the session key, to facilitate deciphering of corresponding frames of the multi-frame video content received from the video source device.

20. The method of claim 19, wherein said generating of successive frame keys comprises generating at each vertical blanking interval of said multi-frame video content, a frame key for deciphering a frame of said multi-frame video content.

21. The method of claim 20, wherein said method further comprises generating a pseudo random bit sequence for each frame, using at least the corresponding frame key, for deciphering the particular frame of said multi-frame video content.

22. The method of claim 21, wherein each of said generating of a pseudo random bit sequence using a corresponding frame key comprises successive modifications of the frame key.

23. The method of claim 22, wherein said successive modifications are performed at horizontal blanking intervals of the frame.

24. The method of claim 21, wherein said method further comprises generating an initial pseudo random bit sequence using at least the session key, and deriving an initial pseudo random number from the initial pseudo random bit sequence to be used with the first frame key to generate a first pseudo random bit sequence to cipher a first frame.

25. The method of claim 21, wherein each of said generating of a pseudo random bit sequence comprises generating sufficient number of pseudo random bits for deciphering a pixel on a bit-wise basis each clock.

26. In a video sink device, a method comprising:

generating a frame key for each frame of a multi-frame video content received from a video source device; and

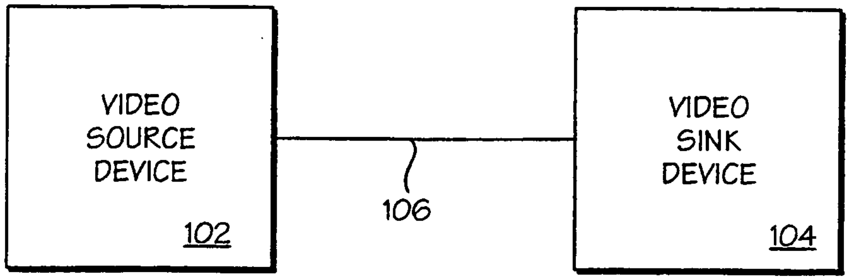

VIDEO SOURCE DEVICE
102
106
VIDEO SINK DEVICE
104

FIG. 1

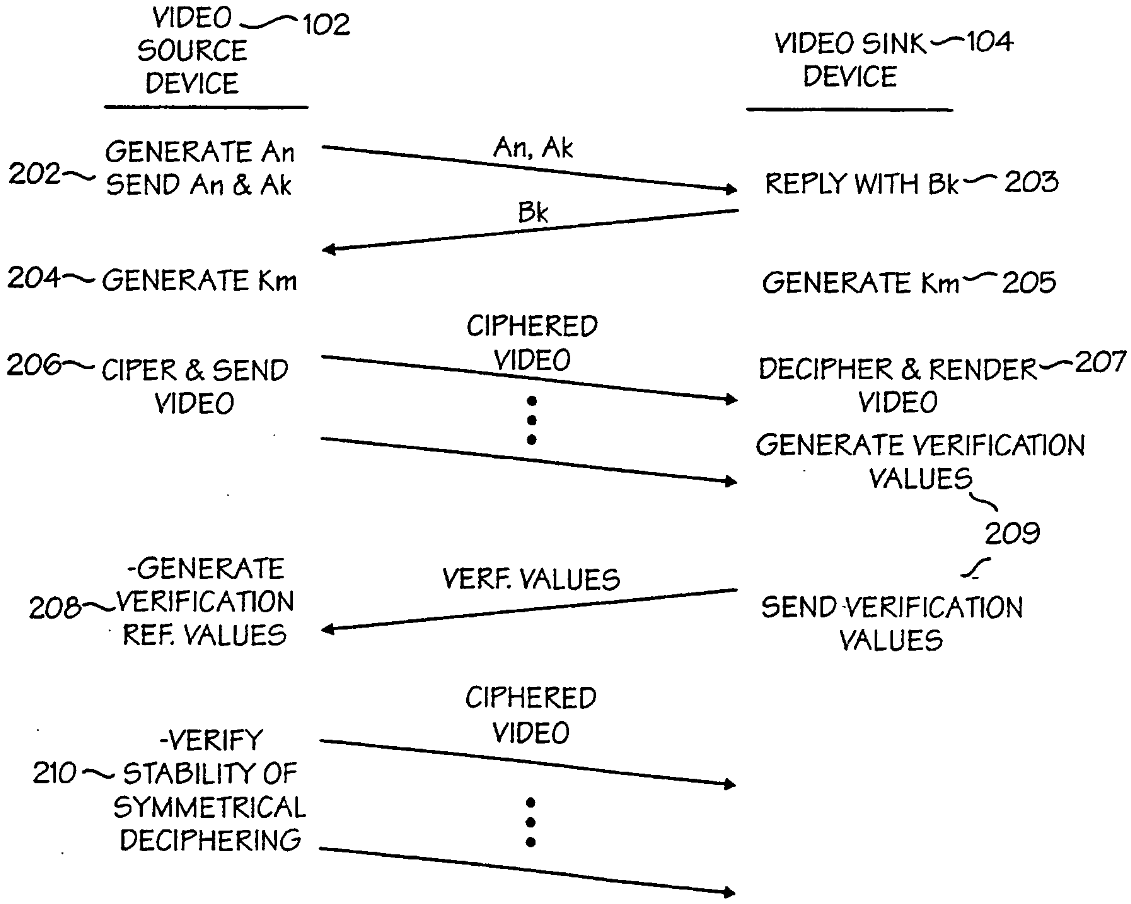

VIDEO SOURCE DEVICE
102
VIDEO SINK DEVICE
104
202
GENERATE An SEND An & Ak
An, Ak
REPLY WITH Bk
203
Bk
204
GENERATE Km
GENERATE Km
205
206
CIPER & SEND VIDEO
CIPHERED VIDEO
DECIPHER & RENDER VIDEO
207
GENERATE VERIFICATION VALUES
209
208
-GENERATE VERIFICATION REF. VALUES
VERF. VALUES
SEND VERIFICATION VALUES
CIPHERED VIDEO
210
-VERIFY STABILITY OF SYMMETRICAL DECIPHERING

FIG. 2

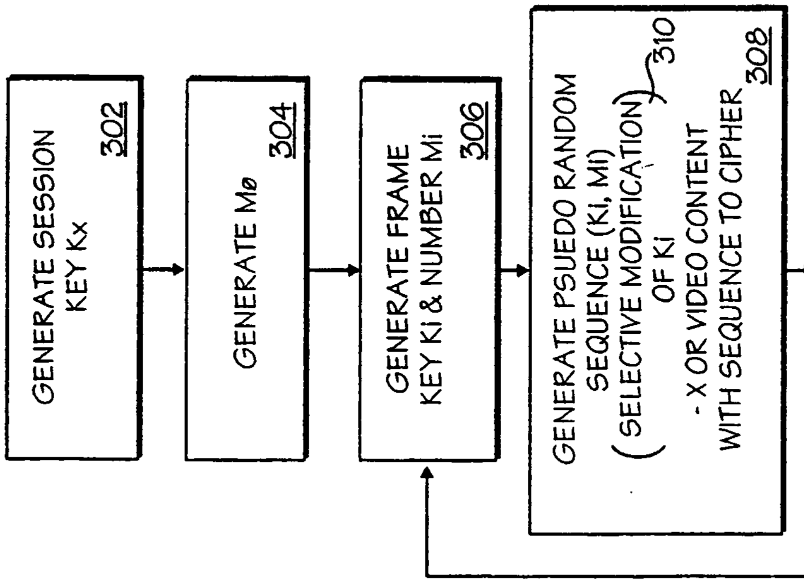

GENERATE SESSION KEY Kx
302
GENERATE Mø
304
GENERATE FRAME KEY Ki & NUMBER Mi
306
GENERATE PSUEDO RANDOM SEQUENCE (Ki, Mi) (SELECTIVE MODIFICATION) OF Ki
310
- X OR VIDEO CONTENT WITH SEQUENCE TO CIPHER
308
MORE ?
YES
NO
END

Fig. 3a

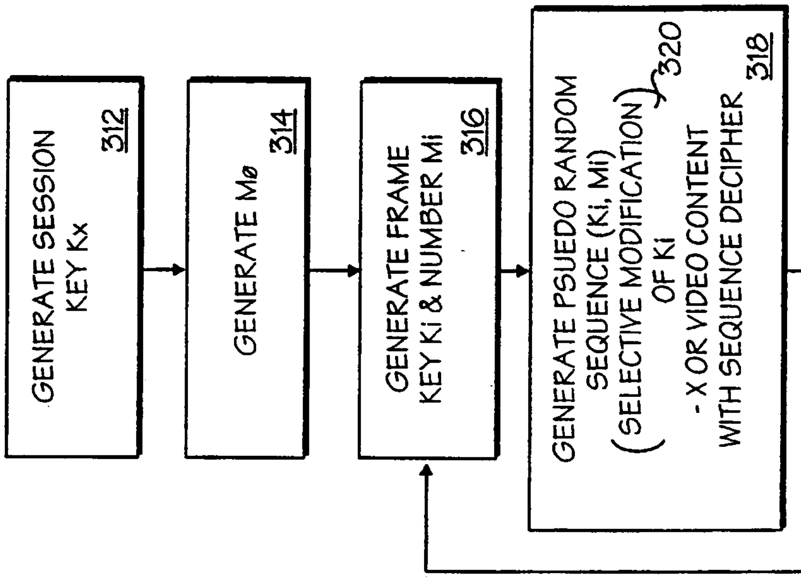

GENERATE SESSION KEY Kx
312
GENERATE Mø
314
GENERATE FRAME KEY Ki & NUMBER Mi
316
GENERATE PSUEDO RANDOM SEQUENCE (Ki, Mi) (SELECTIVE MODIFICATION) OF Ki
320
- X OR VIDEO CONTENT WITH SEQUENCE DECIPHER
318
MORE ?
YES
NO
END

Fig. 3b

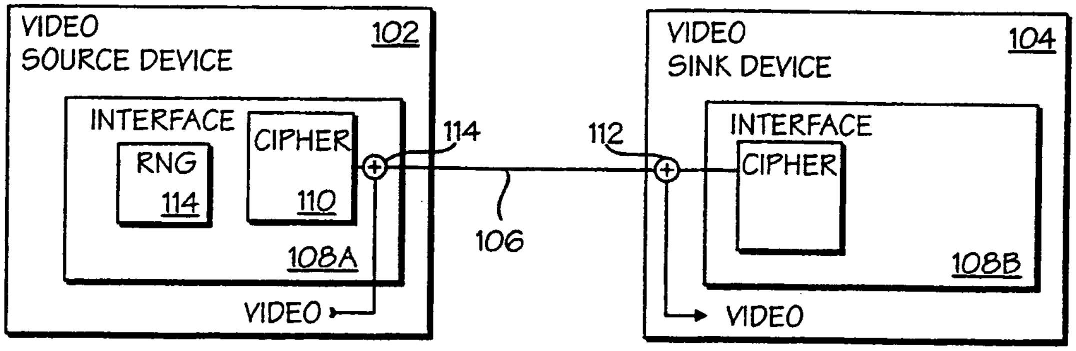

VIDEO
SOURCE DEVICE
102
INTERFACE
RNG
114
CIPHER
110
108A
VIDEO
114
112
106
VIDEO
SINK DEVICE
104
INTERFACE
CIPHER
108B
VIDEO

FIG. 4

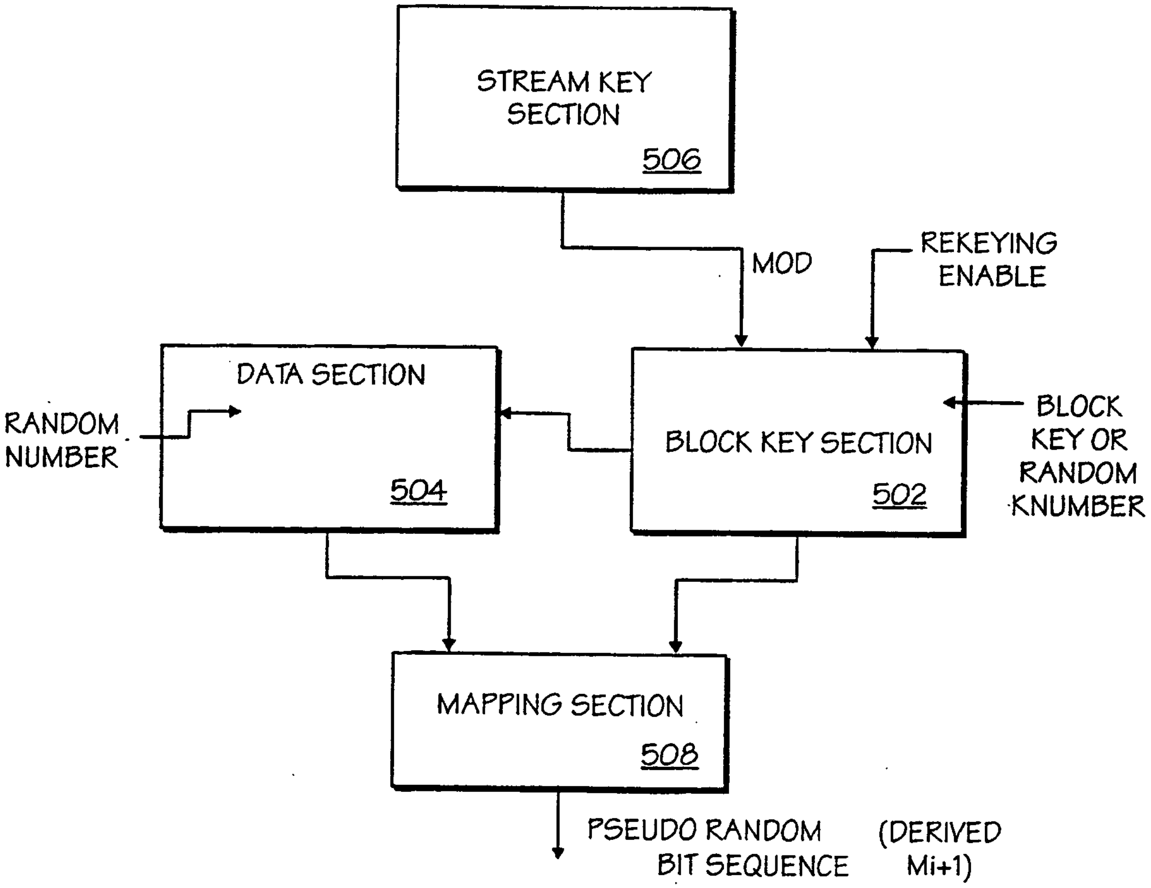

STREAM KEY
SECTION
506
MOD
REKEYING
ENABLE
DATA SECTION
504
RANDOM
NUMBER
BLOCK KEY SECTION
502
BLOCK
KEY OR
RANDOM
KNUMBER
MAPPING SECTION
508
PSEUDO RANDOM
BIT SEQUENCE
(DERIVED
Mi+1)

FIG. 5

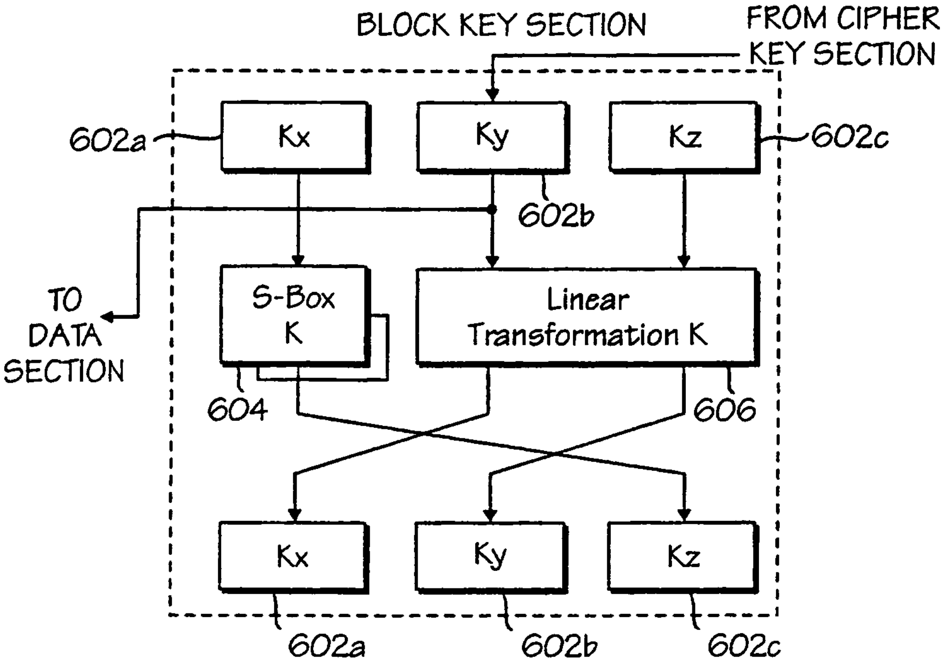

BLOCK KEY SECTION
FROM CIPHER KEY SECTION
602a
Kx
Ky
Kz
602c
602b
TO DATA SECTION
S-Box K
Linear Transformation K
604
606
Kx
Ky
Kz
602a
602b
602c

FIG. 6

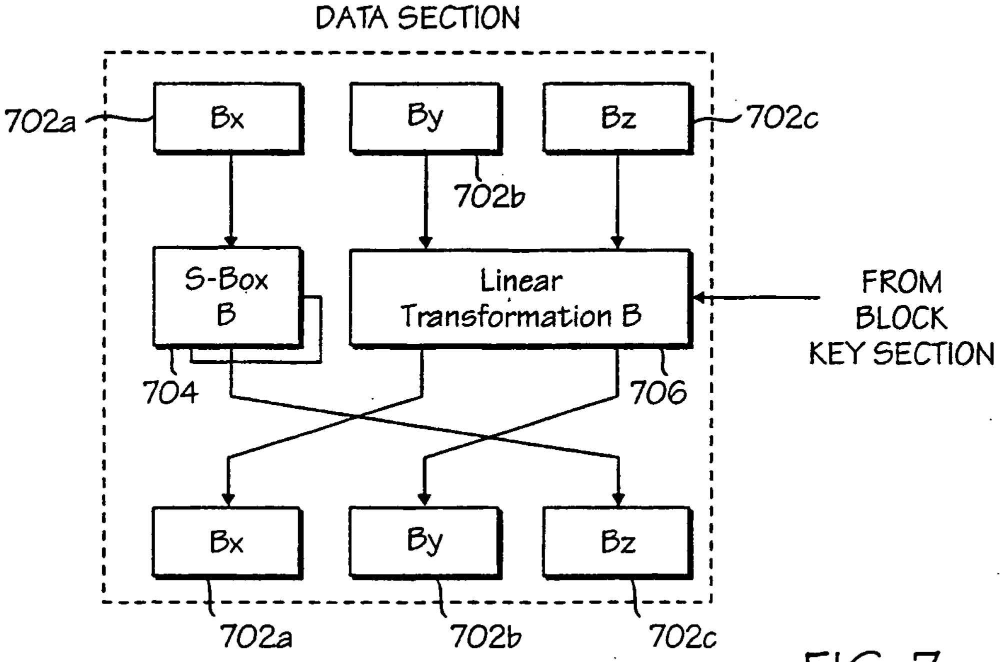

DATA SECTION
702a
Bx
By
Bz
702c
702b
S-Box B
Linear Transformation B
FROM BLOCK KEY SECTION
704
706
Bx
By
Bz
702a
702b
702c

FIG. 7

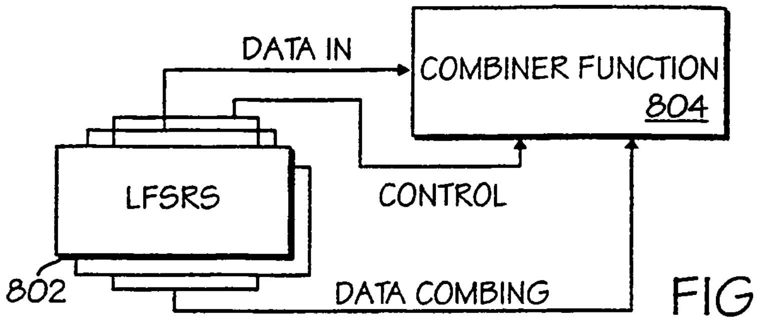


FIG. 8a

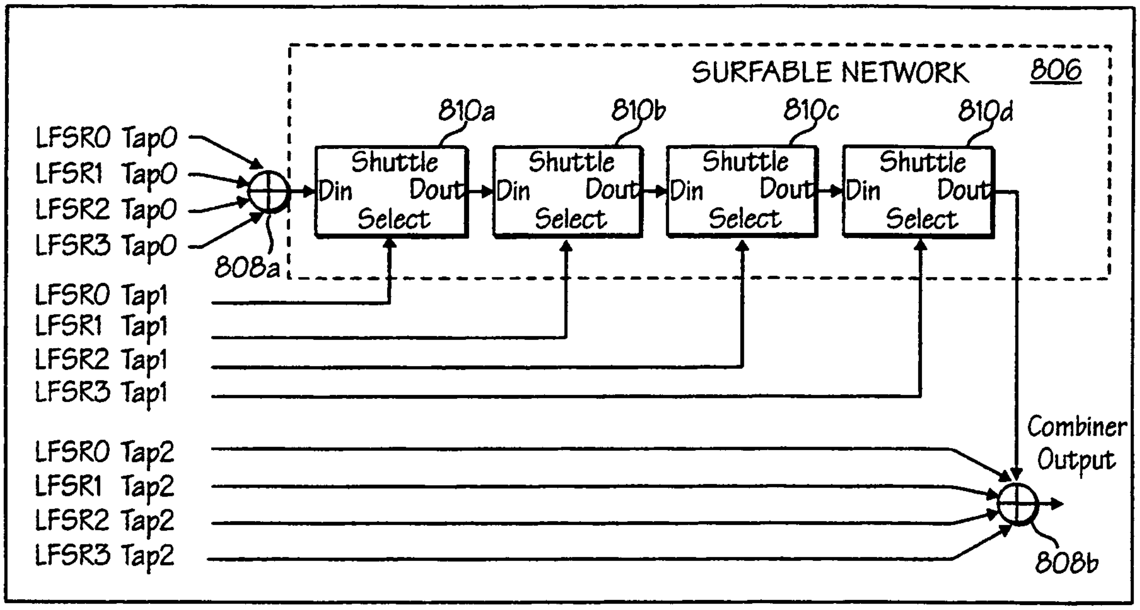


FIG. 8b

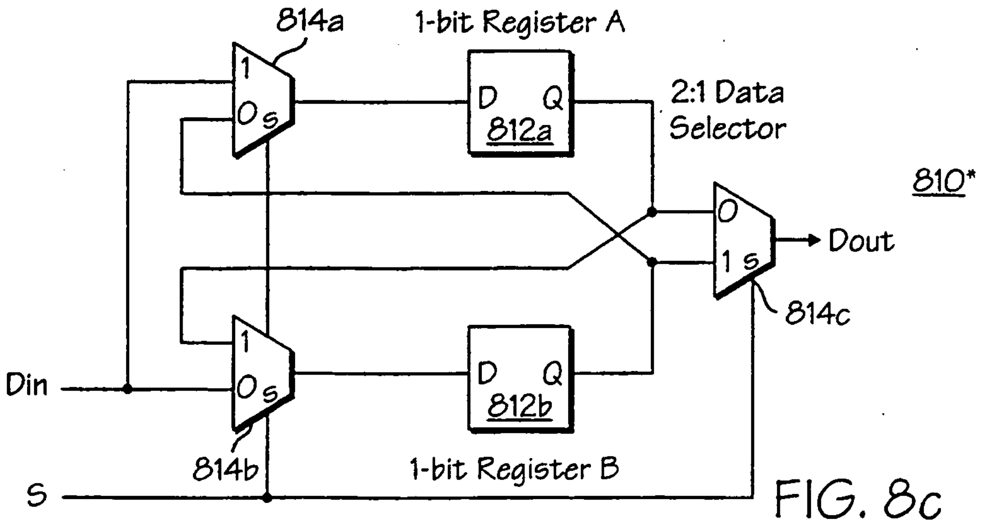


FIG. 8c

INTERNATIONAL SEARCH REPORT

Interr nal Application No
PCT/US 00/22785

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04N7/167

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 99 18729 A (BENARDEAU CHRISTIAN ;CANAL PLUS SA (FR); MAILLARD MICHEL (FR); DAU) 15 April 1999 (1999-04-15) page 7, line 27 - line 30 page 8, line 24 -page 12, line 16 figures 3-5 ---	1-36
A	US 5 621 799 A (IBARAKI SUSUMU ET AL) 15 April 1997 (1997-04-15) column 3, line 3 -column 8, line 19 figures 1-4 ---	1-36
A	US 5 852 472 A (GUTMANN MICHAEL J ET AL) 22 December 1998 (1998-12-22) column 1, line 14-29 figure 3 --- -/--	1,13,19, 26,30,31

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search 29 November 2000	Date of mailing of the international search report 06/12/2000
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Van der Zaal, R

INTERNATIONAL SEARCH REPORT

ormation on patent family members

Interr nal Application No
PCT/US 00/22785

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9918729 A	15-04-1999	AU 9278298 A	27-04-1999
		BR 9812703 A	22-08-2000
		EP 1020080 A	19-07-2000
		NO 20001649 A	02-06-2000
		ZA 9808951 A	12-04-1999
US 5621799 A	15-04-1997	JP 7115414 A	02-05-1995
		JP 7134647 A	23-05-1995
US 5852472 A	22-12-1998	NONE	
US 4953208 A	28-08-1990	JP 2288573 A	28-11-1990
		JP 2810103 B	15-10-1998
		GB 2232032 A,B	28-11-1990